Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
European Journal of Combinatorics 26 (2005) 111–116
European Journal of Combinatorics
www.elsevier.com/locate/ejc

Tests for loop nuclei and a new criterion for a Latin square to be group-based

A.D. Keedwell

University of Surrey, Department of Mathematics and Statistics, GU2 7XH Guildford, Surrey, UK

Received 21 November 2003; accepted 20 January 2004

Available online 17 April 2004

Abstract

We give a new and simple criterion for a Latin square to be group-based and we provide easy-to-implement tests for whether a given element of a loop lies in any one of its three nuclei.

MSC: 05B15; 20N05

Keywords: Latin square; Group; Loop; Nuclei

Two well-known criteria for a Latin square to be group-based are (i) the quadrangle criterion (see, for example, [3]) and (ii) Suschkewitch's test [6]: namely, a Latin square is group-based if the product of the permutations representing every two columns (or rows) is again a permutation representing a column (or row). These two criteria have also been discussed by Siu [4].

In this note, we offer a third criterion which, when implemented by hand, needs fewer tests than either of the foregoing.

Frolov [2] has called a reduced Latin square of order n (with elements $1, 2, \ldots, n$ say) "regular" if the squares obtained by raising each row in turn to the top and then rearranging first the columns and then the remaining rows so that the square is again reduced are all the same.

We shall show as a corollary to the first of our tests for elements of the loop nuclei that a Latin square is regular in this sense if and only if it is group-based and so this gives us a third criterion for deciding whether a given Latin square is isotopic to the multiplication table of a group. This (apparently new) criterion involves only $n/2$ tests at

E-mail address: a.keedwell@eim.surrey.ac.uk (A.D. Keedwell).

0195-6698/$ - see front matter © 2003 Published by Elsevier Ltd
doi:10.1016/j.ejc.2004.01.005

	1	$\cdot$	$\cdot$	b	$\cdot$	$\cdot$	u	$\cdot$
1	1θ	$\cdot$	$\cdot$	$(1\theta)b = 1$	$\cdot$	$\cdot$	$(1\theta)u$	$\cdot$
2	2θ	$\cdot$	$\cdot$	$(2\theta)b = 2$	$\cdot$	$\cdot$	$(2\theta)u$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
x	$x\theta$	$\cdot$	$\cdot$	$(x\theta)b = x$	$\cdot$	$\cdot$	$(x\theta)u$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
n	$n\theta$	$\cdot$	$\cdot$	$(n\theta)b = n$	$\cdot$	$\cdot$	$(n\theta)u$	$\cdot$

Fig. 1. Loop table T after rearranging rows so that the symbols in column b are in natural order.

most as compared to the n^2 tests needed in Suschkewitch's test and the even larger number needed to test the validity of the quadrangle criterion.

Definition. The hth row (column) of the Cayley table of a loop $(Q, \cdot)$ is said to have the *Frolov property* if, when the columns (rows) of the Latin square formed by the body of the table are re-ordered in such a way that the elements of the hth row (column) are in the same order as that of the row (column) border, each row (column) of the re-ordered square coincides with some row (column) of the body of the original Cayley table.

Note that, if every row of a Latin square has the Frolov property, this is equivalent to saying that the Latin square is regular.

Theorem 1. *Suppose that the cell (i, j) of the Cayley table T of the loop $(Q, \cdot)$ contains the entry $a_i b_j$ for $i, j = 1, 2, \ldots, n$, $a_1 = b_1 = e$ where e is the identity element. Then a necessary and sufficient condition that the element b_k belong to the middle nucleus of the loop is that the column of T indexed by b_k has the Frolov property. A necessary and sufficient condition that the element a_h belong to the middle nucleus of the loop is that the row of T indexed by a_h has the Frolov property.*

Proof. We may suppose, without loss of generality, that the symbols used for the loop $(Q, \cdot)$ are $1, 2, \ldots, n$, that 1 is the identity element and that the Cayley table is in reduced form: that is, with the elements of the first row and column in natural order.

Let us suppose that the mapping θ permutes the rows so that the elements $1b, 2b, \ldots, xb, \ldots, nb$ of the column headed by the element b are in the order of the first column: that is, in natural order. Then, $(x\theta)b = x$ for $x = 1, 2, \ldots, n$. (The columns may be rearranged if we wish so that the new square becomes reduced.)

The elements of the column headed by the element u are xu for $x = 1, 2, \ldots, n$. These become $(x\theta)u$ for $x = 1, 2, \ldots, n$ (see Fig. 1). Suppose that this is another column of T for each $u \in Q$. Then, for each $u \in Q$, there exists an element $w \in Q$ such that $(x\theta)u = xw$ for all $x \in Q$, where $(x\theta)b = x$. Thus, $x\theta = xR_b^{-1}$ and so $(xR_b^{-1})u = xw$. Putting $x = b$, we get $u = bw$ or $w = uL_b^{-1}$ so $(xR_b^{-1})u = x(uL_b^{-1})$ for all $x, u \in Q$, or, equivalently, $(xR_b^{-1})(bw) = xw$ for all $x, w \in Q$. If we put $x = yb$, this becomes $y(bw) = (yb)w$ for all $y, w \in Q$. Thus, b lies in the middle nucleus of the loop. □

To prove the second statement, we need only remark that the loop whose rows are the columns of $(Q, \cdot)$ has middle nucleus the same as that of $(Q, \cdot)$.

Corollary. *If and only if a reduced Latin square is regular, it is group-based.*

Proof. If and only if all rows of a reduced Latin square have the Frolov property, the Cayley table obtained by bordering it by its own first row and column represents a loop $(Q, \cdot)$ whose middle nucleus is the whole of Q and so $(Q, \cdot)$ is a group. □

Remark. If p is the smallest prime which divides the order $|Q|$ of a loop $(Q, \cdot)$ (or reduced Latin square L formed by its Cayley table) and if $|Q|/p$ rows, excluding the first, of L have the Frolov property, this is sufficient to ensure that L is group-based since it ensures that at least $1 + (|Q|/p)$ elements of Q are in the middle nucleus of $(Q, \cdot)$. The latter has order which divides Q: that is, it has order at most $|Q|/p$ if it is not the whole of Q.

(Note that, in particular, for a Latin square of odd order, it is sufficient that at most a third of the rows have the Frolov property to be sure that the square is group-based. For a square of prime order, just one row is sufficient.)

We can adapt Suschkewitch's criterion to obtain another test for an element to belong to the middle nucleus of a loop, as follows.

Theorem 2. *Suppose that the cell (i, j) of the Cayley table T of the loop $(Q, \cdot)$ contains the entry $a_i b_j$ for $i, j = 1, 2, \ldots, n$, $a_1 = b_1 = e$, where e is the identity element. Then a necessary and sufficient condition that the element b_k belong to the middle nucleus of the loop is that the product of the permutation which represents the column headed by b_k by each one of the permutations which represent the remaining columns (and by itself) is again a permutation representing a column.*

Proof. As before, we may suppose without loss of generality that the symbols used for the loop $(Q, \cdot)$ are $1, 2, \ldots, n$, that 1 is the identity element and that the Cayley table is in reduced form: that is, with the elements of the first row and column in natural order. The column headed by the element b is then represented by the permutation $R_b : x \to xb$ from natural order. Each other column is similarly represented by a permutation $R_u : x \to xu$. We suppose that every product $R_b R_u$ is again a permutation, say R_v, representing some column of the Cayley table. Then $x R_b R_u = x R_v$ for all $x \in Q$. This is true in particular when $x = 1$, so $v = bu$. But then $x R_b R_u = x R_{bu}$ for all $x, u \in Q$. That is, $(xb)u = x(bu)$. Thus, b is an element of the middle nucleus of the loop. □

Note that Theorem 2 requires n tests to test for each element of the middle nucleus as compared to only one needed for the test of Theorem 1.

It seems reasonable to expect that tests for elements of the left and right nuclei, analogous to those given in Theorem 1 for elements of the middle nucleus but involving permutation of symbols rather than rows or columns, should exist. We show in Theorem 3 below that this is the case.

Definition. The hth column of the Cayley table of a loop $(Q, \cdot)$ is said to have the F^*-*property* if, when the symbols of the Latin square formed by the body of the table are re-ordered in such a way that the elements of the hth column are in the same order as that

of the column border, each column of the re-ordered square coincides with some column of the body of the original Cayley table.

Theorem 3. *Suppose that the cell (i, j) of the Cayley table T of the loop $(Q, \cdot)$ contains the entry $a_i b_j$ for $i, j = 1, 2, \ldots, n$, $a_1 = b_1 = e$, where e is the identity element. Then, if the column of T indexed by b_k has the F^*-property, the element b_k belongs to the right nucleus of the loop. If the row of T indexed by a_h has the F^*-property, the element a_h belongs to the left nucleus of the loop.*

Proof. As before, we may suppose without loss of generality that the symbols used for the loop $(Q, \cdot)$ are $1, 2, \ldots, n$, that 1 is the identity element and that the Cayley table is in reduced form. The elements of the column headed by the element b take the form xb for $x = 1, 2, \ldots, n$. To permute the symbols so that these are in natural order, we multiply each symbol by R_b^{-1}.

The elements of the column headed by the element c are xc for $x = 1, 2, \ldots, n$. These become $(xc)R_b^{-1}$ for $x = 1, 2, \ldots, n$. Suppose that this is another column of T for each $c \in Q$. Then, for each $c \in Q$, there exists an element $d \in Q$ such that $(xc)R_b^{-1} = xd$ for all $x \in Q$. In particular, $(1c)R_b^{-1} = 1d$ and so $d = cR_b^{-1}$. Thus, $(xc)R_b^{-1} = x(cR_b^{-1})$ for all $x, c \in Q$.

We have $c = dR_b$. Then $[x(dR_b)]R_b^{-1} = xd$. That is $x(dR_b) = (xd)R_b$ or $x(db) = (xd)b$ for all $x, d \in Q$, whence we conclude that b is in the right nucleus of the loop.

To prove the second statement, we use the fact that the loop whose rows are the columns of $(Q, \cdot)$ has left nucleus equal to the right nucleus of $(Q, \cdot)$. □

We may ask "What is the smallest order n for which loops with non-trivial left, right or middle nuclei exist?" Since the orders of the nuclei divide the order of the loop and since loops of order four are groups, $n \geq 6$. There exists a proper conjugacy-closed loop of order six and, for such a loop $(Q, \cdot)$, Q/N is an Abelian group so the nucleus N must be non-trivial. In fact, there are four isomorphically distinct loops of order six which have non-trivial nuclei. Interestingly, there is also one whose left, right and middle nuclei are all different and intersect only trivially.[1] Eight is the smallest order for which Bol loops exist (see [1]) and one at least of these has both a non-trivial nucleus and left and right nuclei which are distinct. For the interest of the reader, we give the Cayley tables of these minimal order loops in Fig. 2.

Next, we show that a test involving permutation of symbols can be used to test whether a particular element of a loop satisfies the law of right (or left) permutability (see [5, p. 154], or [3, p. 59]).

Theorem 4. *Suppose that the cell (i, j) of the Cayley table T of the loop $(Q, \cdot)$ contains the entry $a_i b_j$ for $i, j = 1, 2, \ldots, n$, $a_1 = b_1 = e$, where e is the identity element and suppose that, when the symbols in the Latin square L which forms the body of the Cayley table are permuted so that the column of T indexed by b is in natural order, every row of the new Latin square L' coincides with some row of L. Then the element b satisfies the law of right permutability: namely, $(ab)c = (ac)b$ for all $a, c \in Q$.*

[1] This information was kindly supplied by M.K. Kinyon.

Proof. As before, we may suppose that the symbols used for the loop $(Q, \cdot)$ are $1, 2, \ldots, n$, that 1 is the identity element and that the Cayley table is in reduced form. The elements of the column headed by the element b take the form xb for $x = 1, 2, \ldots, n$. To permute the symbols so that these are in natural order, we multiply each symbol by R_b^{-1} as in Theorem 3.

The elements of the row indexed by the element u are ux for $x = 1, 2, \ldots, n$. These become $(ux)R_b^{-1}$ for $x = 1, 2, \ldots, n$. Suppose that this is another row of T for each $u \in Q$. Then, for each $u \in Q$, there exists an element $v \in Q$ such that $(ux)R_b^{-1} = vx$ for all $x \in Q$. In particular, $(u1)R_b^{-1} = v1$ and so $v = uR_b^{-1}$. Thus, $(ux)R_b^{-1} = (uR_b^{-1})x$ for all $x, u \in Q$.

We have $u = vR_b$. Then, $[(vR_b)x]R_b^{-1} = vx$. That is, $(vR_b)x = (vx)R_b$ or $(vb)x = (vx)b$ for all $x, v \in Q$, whence we conclude that the element b satisfies the law of right permutability. □

Remark. It is necessary to remember here that Belousov has proved that a quasigroup or loop whose elements satisfy any irreducible balanced identity is isotopic to a group (see p. 68 of [3] for details). The law of right permutability is such a balanced identity so, if every column of T has the property described in Theorem 4, then $(Q, \cdot)$ is isotopic to an Abelian group.[2]

Finally, we can use the above results to obtain another simple test for a group to be group-based and one which simultaneously determines whether the group is Abelian.

Definition. The hth column of the Cayley table of a loop $(Q, \cdot)$ is said to have the F_a^*-*property* if, when the symbols of the Latin square formed by the body of the table are re-ordered in such a way that the elements of the hth column are in the same order as that of the column border, each column of the re-ordered square coincides with some column of the body of the original Cayley table and also each row of the re-ordered square coincides with some row of the original one.

Theorem 5. *If (and only if) each column of the Cayley table T of a loop $(Q, \cdot)$ has the F_a^*-property, $(Q, \cdot)$ is an Abelian group.*

Proof. By Theorem 4, all triads of elements satisfy the law of right permutability $(ab)c = (ac)b$. Putting $a = 1$, we get $bc = cb$ and so the commutative law holds. It then follows that $c(ab) = (ca)b$.

Conversely, if $(Q, \cdot)$ is an Abelian group, Theorems 3 and 4 together imply that the F_a^*-property holds. □

Corollary. *If and only if each column of a reduced Latin square L has the F^*-property, L is based on a group and, if and only if each column has the stronger F_a^*-property, this group is Abelian.*

[2] For a loop $(Q, \cdot)$ which satisfies the law of right permutability $(ab)c = (ac)b$ for all $a, b, c \in Q$, we may prove directly that it is isomorphic to an Abelian group as in the proof of Theorem 5.

(a)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	6	5	2	1	3
5	5	4	6	3	2	1
6	6	5	4	1	3	2

(b)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	5	1	6	4	2
4	4	6	2	5	3	1
5	5	4	6	2	1	3
6	6	3	5	1	2	4

(c)

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	8	6	1	7	3	5	4
3	3	7	8	6	1	4	2	5
4	4	1	7	8	6	5	3	2
5	5	6	1	7	8	2	4	3
6	6	3	4	5	2	8	1	7
7	7	5	2	3	4	1	8	6
8	8	4	5	2	3	7	6	1

Fig. 2. (a) The nucleus of this conjugacy-closed loop is $N = \{1, 2, 3\}$. (b) The nuclei of this loop are $N_i = \{1, 2\}$, $N_m = \{1, 5\}$, $N_r = \{1, 3\}$. (c) The nuclei of this Bol loop are $N_l = \{1, 6, 7, 8\}$, $N_m = N_r = \{1, 8\}$.

Acknowledgement

The author wishes to thank Michael Kinyon for much valuable information concerning loops of small order.

References

[1] R.P. Burn, The smallest Bol loops, Math. Proc. Cambridge Philos. Soc. 84 (1978) 377–385.
[2] M. Frolov, Recherches sur les permutations carrés, J. Math. Spéc. (3) 4 (1890) 25–30.
[3] J. Dénes, A.D. Keedwell, Latin Squares and their Applications, Académiai Kiadó, Budapest, 1974.
[4] M.-K. Siu, Which Latin squares are Cayley tables?, Amer. Math. Monthly 98 (1991) 625–627.
[5] A. Sade, Quasigroupes obéissant à certaines lois, Rev. Fac. Sci. Univ. Istambul. Sér. A 22 (1957) 151–184.
[6] A. Suschkewitch, On a generalization of the associative law, Trans. Amer. Math. Soc. 31 (1929) 204–214.